WEDDS: The WITS Encrypted Data Delivery System[1]

Jeffrey S. Norris
Jet Propulsion Laboratory
4800 Oak Grove Drive
Mail Stop 198-221
Pasadena, CA 91109
818-354-5472
Jeffrey.S.Norris@jpl.nasa.gov

Paul G. Backes
Jet Propulsion Laboratory
4800 Oak Grove Drive
Mail Stop 198-221
Pasadena, CA 91109
818-354-3850
Paul.G.Backes@jpl.nasa.gov

Abstract—WEDDS, the WITS Encrypted Data Delivery System, is a framework for supporting distributed mission operations by automatically transferring sensitive mission data in a secure and efficient manner to and from remote mission participants over the Internet. WEDDS was originally developed as part of WITS, the Web Interface for Telescience, and will be used in the 1998 Mars Polar Lander Mission to support distributed mission operations over the Internet for the first time in NASA history. WEDDS is written in Java, and is designed to provide secure distributed operations capabilities to any existing mission application with little modification, and in a manner that is nearly transparent to the existing application and its users.

WEDDS relies on the NASA Public Key Infrastructure (PKI) to verify the identity of remote users. Remote users must apply in person at a NASA security office or another trusted security authority in order to receive a digital certificate. All connections are made using the Secure Sockets Layer (SSL) protocol in conjunction with the user's certificate, and all transmissions are protected against eavesdropping through encryption with the Triple-DES-EDE3 algorithm.

TABLE OF CONTENTS

1. INTRODUCTION

Nearly every NASA mission is faced with a difficult problem. Every day, a large amount of data is received from a spacecraft at a mission operations center and placed into a local database for processing and viewing by mission scientists. Unfortunately, these scientists can't always be at the mission operations center for the duration of the mission, and so a secure and efficient way to deliver data to remote scientists is needed. To make the problem more complex, a particular scientist may only be interested in or be allowed to access to a small fraction of the data delivered from the spacecraft. Because this data is often quite sensitive, missions often choose not to deliver data to many of these remote scientists at all. This greatly degrades the efficiency of mission operations and often forces mission scientists to stay at the mission operations center for the duration of a mission.

To enable collaboration in daily sequence generation by distant, Internet-based scientists, a secure and efficient way to deliver mission data to remote scientists is needed. Furthermore, a subset of those remote scientists should be able to securely transfer data and commands back to the mission control center. WEDDS, the WITS (Web Interface for Telescience) Encrypted Data Delivery System, was designed to provide this capability for a variety of existing mission applications in a secure, efficient, and transparent manner. WEDDS was originally developed as part of WITS, and will be used in the 1998 Mars Polar Lander Mission to support distributed mission operations over the Internet for the first time in NASA history. WITS' support for distributed operations in the Mars Polar Lander Mission is discussed in detail in a companion paper [1].

This paper begins with a list of ten requirements that a secure and efficient data distribution system should meet. Next is a brief discussion of several approaches that were considered and eventually discarded in favor of WEDDS' final implementation. A detailed description of the design and operation of WEDDS follows, with particular attention paid to its integration with WITS for the Mars Polar Lander mission. The paper concludes with a discussion of the security approach used by WEDDS and a verification of WEDDS with respect to the requirements specified at the beginning of the paper.

2. SPECIFICATION OF SYSTEM REQUIREMENTS

Through many discussions with several security experts at JPL and UCLA, as well as the mission system administrators for the Cassini and Mars Polar Lander missions, a list of requirements for a secure data distribution

[1] 0-7803-5846-5/00/$10.00 © 2000 IEEE

system were compiled. These requirements, listed below, form the basis for the design of WEDDS.

Security Requirements

1. **Strong Authentication:** The identities of the remote user and server must be reliably established before any data is transferred.
2. **Strong Encryption:** The data must be encrypted while in transit to protect against eavesdropping or "packet-sniffing" attacks.
3. **Fine Grain Access Control:** Individual scientists may want, or have authorization for, only a specific subset of the downlink data. Access should be controlled on a file by file, user by user basis.
4. **Minimal Impact to Operations Center Security:** The introduction of the system should not significantly decrease the level of security at the mission operations center. If a hacker compromises the delivery system, he should not be able to infiltrate the operations center computers.

Efficiency Requirements

5. **Bandwidth Efficiency:** Data should be compressed and delivered in large packages to reduce transmission time. The system should not require remote users to be constantly connected.
6. **Transparency:** The system should deliver the data automatically and silently, without requiring much effort on the part of the remote user or the mission system administrator.
7. **Platform Independence**: The system must be compatible with all major computer platforms without modification.
8. **Multiple Application Support**: Once the system is completed, it should be able to deliver data for a variety of mission applications.
9. **Scalability**: It should be easy to add additional users to the system, and system performance should degrade gracefully as the number of users grows.
10. **Support for two-way communication**: The system should support, if desired, a secure method for remote users to transmit data back to the mission control center.

Requirements 1 through 4 deal with the security of the system, while 5 through 10 require the system to operate efficiently. WEDDS was designed to meet all of these expectations, and its performance with respect to these requirements is discussed in section 6 of this paper.

3. Existing Approaches Considered

Several existing approaches to automatic, secure data delivery were considered before WEDDS was created. This section discusses the relative merits and shortcomings of these approaches with respect to the requirements listed in the last section.

Dedicated Leased Lines

Dedicated leased lines are the current approach used for the transfer of sensitive mission data to SOPC's, Science Operations and Planning Computers. SOPC's are dedicated computers, located at a mission scientist's home institution, which allow a limited amount of distributed operations for JPL missions. Every SOPC must be connected via its own leased line to NASCOM (Nasa Communications), a wide area network (WAN) consisting of leased lines purchased and maintained by NASA [2]. While dedicated leased lines have been the best solution for NASA ground communications in the past, the continuing maintenance of a wide area network for NASA is very expensive. For instance, according to the system administrators of the Cassini mission, the maintenance of the leased lines for the mission's 13 remote sites cost roughly five to six million dollars per year, and this cost grows significantly with every additional user of the system. This expense seems very high when it is considered that, used alone, dedicated leased lines don't meet any of the requirements specified in section 2 for a secure distribution network, and only meet half of the requirements for an efficient system.

NASCOM is currently engaged in studies to determine the viability of using the Internet for NASA ground communications instead of the current leased wide area network. While it may seem risky to use a public medium for mission sensitive data, it should be noted that NASCOM currently applies no encryption or authentication to the data transferred over its wires, relying instead upon the telephone companies to prevent an unauthorized party from tapping into the leased line. Unfortunately, the task of policing every piece of wire in a wide area network as gigantic as NASCOM is simply infeasible. Even if dedicated leased lines continue to be used for NASCOM's transport medium, a system like WEDDS still needs to be installed to use the medium securely and efficiently.

It has been argued that dedicated leased lines are more reliable than the Internet because the lines are not shared with the public, but in fact, the Internet's highly redundant structure greatly increases the reliability of the connection between the mission operations center and the remote site.

Virtual Private Networks

Virtual Private Networks (VPN's) allow a file system to be shared through an encrypted connection, often called a "tunnel." JPL uses a virtual private network to allow JPL employees to securely access files on their work computers from home. VPN's satisfy requirements 3,6,7,8,9, and 10 from above, but fall short on 1,2,4, and 5.

1,2: Weaker authentication and encryption--Most VPN's do not use an authentication and encryption method as aggressive as WEDDS' algorithms. Many rely on DES encryption, which has been shown to be easily broken using specialized hardware [3], and user authentication is accomplished through a password alone, instead of a

password paired with a digital certificate file, as is the case with WEDDS.

4: Significant Impact to Operations Center Security—VPN's are a more general and complex tool that typically give more access to remote users than is desired for simple data distribution. They are built on the principle that the remote user's network should appear to be part of the mission control center's network. This is a dangerous amount of access to allow to a remote network that is not entirely trusted. Furthermore, the increased complexity of this system makes it more susceptible to exploitation. Finally, if a user were able to compromise the VPN's security, they could conceivably gain access to mission resources outside of the data distribution system.

6: Poor Transparency—Even though most VPN's use compression to better utilize available bandwidth, they don't automatically transfer data to the remote user's machine. The user must locate the data they are interested in, request the data, and then wait for it to be delivered. So, even if a VPN is used to provide encryption and compression, a delivery mechanism like WEDDS is still needed to automatically retrieve the correct data for a user.

Secure Login Applications

Some departments at JPL that deal with sensitive mission data have elected to use encrypted login programs like *ssh* (Secure Shell) to allow users to connect to machines with the sensitive data remotely. While *ssh* does apply a strong form of encryption to the transmissions, satisfying requirement 2, the authentication model used by *ssh* is inherently weaker than the model used by WEDDS because it depends on a user password alone, rather than a user password and a digital certificate file. *Ssh* satisfies requirements 2,3,5,7,8, 9, and 10 from section 2, but fails to meet 4 and 6.

4: Significant Impact to Operations Center Security-- if an unauthorized user manages to connect via *ssh* to the mission operations center, then they have **login access** to a mission critical machine—a very dangerous situation. New security exploits are discovered weekly that allow hackers who have managed to gain basic login access to a machine to give themselves super-user access. This problem is shared by the VPN approach above.

6: Poor Transparency--Ssh suffers from the same problem described in the VPN section above- the data isn't actually delivered to the remote user's machine unless they use a tool to transfer it manually. This requires every remote user to know where to find their data, when the data has been updated, and where to put the data on their own system. A mission using *ssh* as its delivery mechanism will have a difficult time determining if its remote users are up to date, and the remote users will likely become frustrated with the complexity of the delivery process.

4. Design and Operation of WEDDS

In this section, the overall design of WEDDS will be described by discussing its installation and operation in the Mars Polar Lander Mission. In the interest of clarity, the security of the system will not be explored in detail here. The next section will focus on the details of the approach to security used in WEDDS.

WEDDS is implemented as two Java programs, a server and a client. For each mission, there is typically one server, operating behind a mission firewall, and many clients, one on each remote user's machine. WEDDS relies on the Entrust Java Toolkit for many low-level encryption and authentication commands. The Entrust Corporation, the provider of NASA's public key infrastructure, provides the Entrust Java Toolkit free of charge [4].

Figure 1 illustrates how the WEDDS server and client will operate during the Mars Polar Lander (MPL) mission. Data is received at JPL from the lander via the Deep Space Network and is sent to a UCLA SOPC (Science Operations and Planning Computer) via a dedicated leased line. The data is then extensively processed and saved in formats that can be read by the MPL mission planning tools, such as WITS, the Web Interface for Telescience, which WEDDS was designed to support. While local operations staff are using WITS to view downlink data and generate new sequences for the lander, a WEDDS administrator adds the new processed downlink data to the data that WEDDS is distributing to remote users. The WEDDS server then waits for a remote WEDDS client to initiate an update request to the WEDDS server. Note that the remote user does not need to initiate this action, it is performed periodically by the WEDDS client software.

When a WEDDS client initiates an update request, no trust has been established between the client and the server. In other words, the WEDDS server can not be certain that a legitimate client is requesting data, and the remote client has not confirmed that it is actually connected to the WEDDS server. In order to satisfy both of them, a process called SSL (Secure Sockets Layer) authentication takes place. The SSL authentication process is described in detail in the next section.

Once the server has confirmed the identity of the client and vice-versa, the client provides information to the server regarding the last update that the client received. The server checks to see if new data has become available since the client's last update, and sends the new data if any exists. The transmission of the data, as is the case with all transmissions between the client and the server, is encrypted. Once the update has completely arrived at the client's machine, the data is automatically decompressed and placed into the proper directories on the remote user's computer.

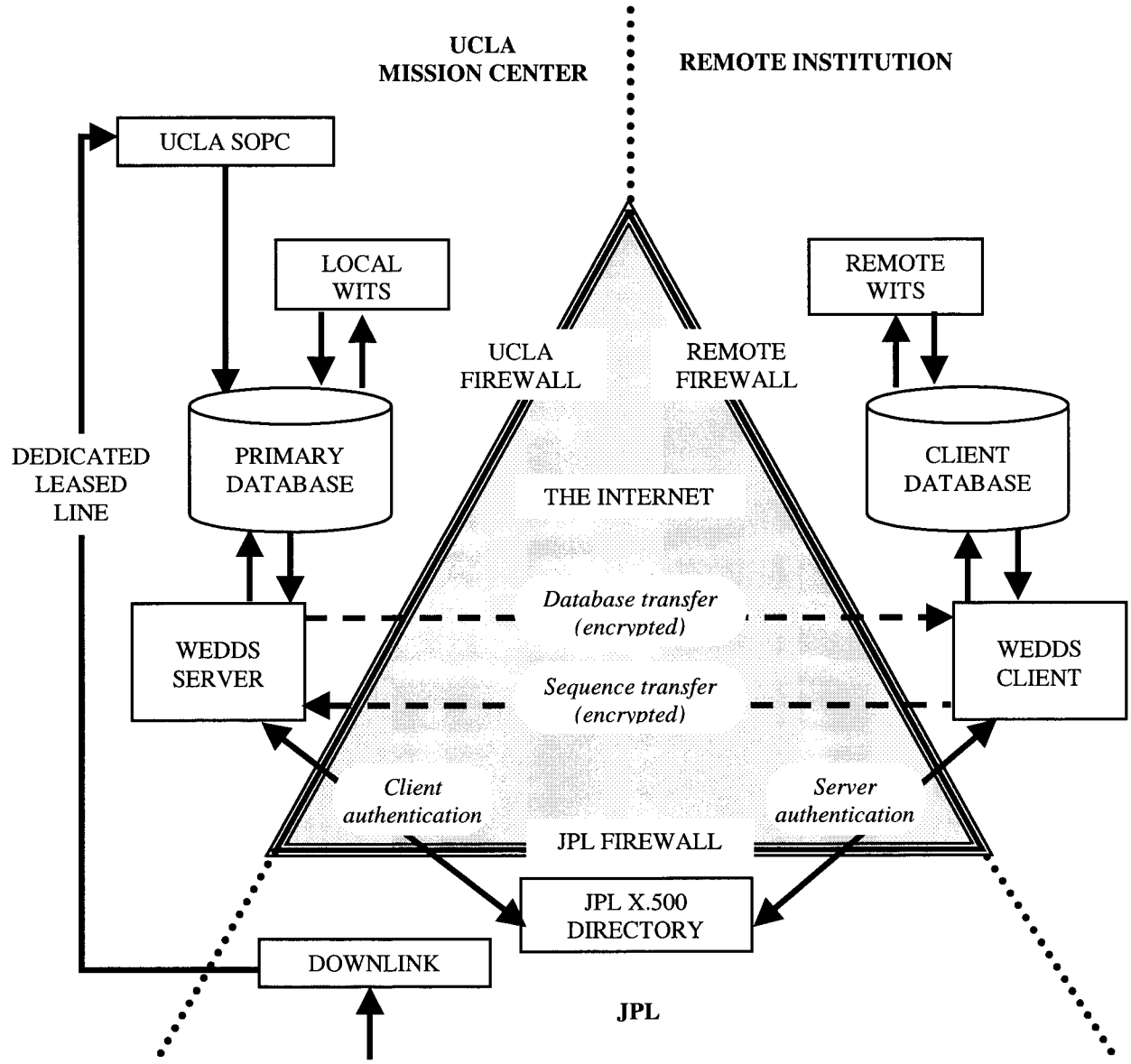

Figure 1 Installation of WEDDS for the Mars Polar Lander Mission

At this point, the remote user can operate on the data using WITS or any other mission tool as if he were at the mission operations center. In fact, when WITS is run at a remote site, the software doesn't actually realize that it isn't at the mission operations center—the same piece of software is used. This is important to mention because WEDDS has made it possible for the same piece of software to run at the mission operations center or remotely without any modification.

Ordinarily, when it is time for a remote user to return a command sequence to the mission operations center, the user would simply save the sequence in a specific directory and WEDDS would transfer it to the correct directory at the mission operations center. However, since WEDDS has been integrated into WITS for the Mars Polar Lander mission, WITS actually uses the encrypted connection set up by WEDDS to communicate directly with a server at UCLA that handles remote sequence submission. When a sequence arrives at the mission operations center at UCLA, it is always verified by an operator at UCLA before it is integrated into the actual mission plan. This final check ensures that the sequence that was generated is legitimate.

5. Details of WEDDS' approach to security

WEDDS's security strategy can be broken down into three parts: Registration, Authentication, and Encryption. These steps are illustrated in figure 2 and are described in detail below.

Registration

Every remote user of WEDDS must have two things to initiate any connection to the server: a certificate disk, and the password to that certificate disk. The certificate disk contains the user's private signing key and private

encryption key, which are needed to positively prove that user's identity to the WEDDS server over the Internet. The disk alone can not be used to connect to the server without the user's password, and the user's password is useless without the certificate disk. The certificate disk is a 3.5" floppy disk, and the user is instructed to keep the disk in a secure place and never place its files onto a hard drive. The technology is also available to record the certificate onto a "smart card", which acts exactly like the floppy certificate disk except that the data on the smart card can not be easily copied from the card.

In order to receive a certificate disk, a remote user must go through a registration process, shown in steps 1 and 2 of figure 2. First, they must appear, in person, at a NASA center security office, or at another trusted institution's security office (a university, for instance.) They provide two forms of identification to a specially trained "registration authority" (RA), who confirms their identity and gives them two numbers that can be used to create the certificate disk. In the generation of the certificate disk, the user specifies a password. Once this process is complete, information is placed in JPL's X.500 directory that the WEDDS server will use to verify the identity of the user in the Authentication stage.

Next, the user must contact the mission system administrator, who instructs the WEDDS server to allow that user remote access. Note that the WEDDS server is also issued a certificate disk by the JPL Public Key Infrastructure (PKI), which it uses to prove its identity to remote users.

Authentication

Steps 3 through 9 in figure 2 are repeated for every transmission from the client to the server or from the server to the client. In steps 3 through 7, the server and client exchange digital "signatures", which they generate from the data on their certificate disks. They verify these signatures by communicating with the JPL X.500 directory. This process, SSL authentication, relies on the fact that it is nearly impossible for someone to generate another user's digital signature without that user's certificate disk and password. In order for an unauthorized user gain access to the server, he must either steal a legitimate user's certificate disk and password, or compromise the NASA certificate authority (CA), the system that issues certificates to users. The NASA CA is highly protected, and forms the backbone for NASA approach to data security in the future. A more detailed description of the SSL authentication process is found online in the Netscape Corporation's specification for the SSL algorithm [5].

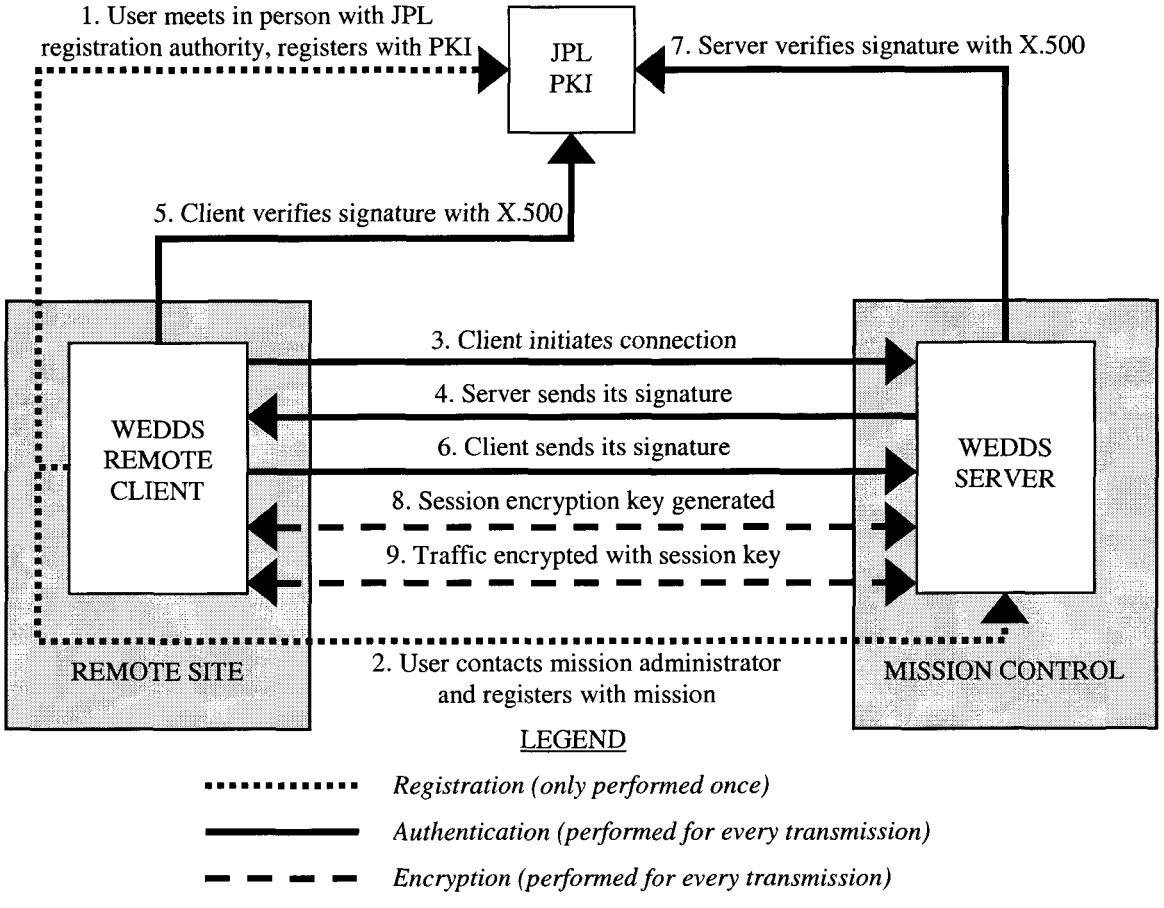

Figure 2 Steps required for a remote user to securely retrieve data from WEDDS'

Encryption

In step 8, the last step in establishing a connection, the client and server generate a unique symmetric encryption key set that will be used in the Triple-DES-EDE3 encryption algorithm to encrypt the traffic for this transaction. This encryption key is decided upon using the Diffie-Hellman key agreement protocol, which is an algorithm that allows two parties to agree upon a secret encryption key without ever transmitting that key in clear-text over the Internet [6]. After an encryption key has been agreed upon, all subsequent traffic for this transaction is encrypted. This encryption makes WEDDS transactions invulnerable to eavesdropping or "packet-sniffing" attacks. To increase the security of the transmissions, a new encryption key protects every subsequent WEDDS transaction. Even if an attacker managed to compromise an encryption key (a highly unlikely accomplishment), he would only have access to the data in a single transmission.

6. Verification of System Requirements

In section 2, ten requirements for a mission data distribution system were established. It is worthwhile to describe how WEDDS meets each of these requirements.

Strong Authentication—WEDDS works within the NASA Public Key Infrastructure (PKI), which is currently being deployed at several NASA centers. A PKI is a system that allows multiple users to securely establish their identity over the Internet, and encrypt data so that only the intended recipient can decipher it. Public Key Cryptography, the backbone of every PKI, was developed by Rivest, Shamir, and Adleman at MIT in 1977 [7]. WEDDS uses the SSL (Secure Sockets Layer) protocol to perform authentication, a highly secure approach that is used to protect nearly every online commerce transaction today [5]. In order for a user to complete the authentication process, he must provide both the digital certificate disk he received upon registration and his password. This is more a more secure approach than a password-only system.

Strong Encryption—Data transmitted by WEDDS is encrypted using the Triple-DES-EDE3 algorithm. Breaking this encryption method, even if every computer in the world were used, would take millions of years [8]. WEDDS generates a new encryption key set for this algorithm for **every transmission** between the server and a client. Therefore, if a hacker did manage to "get lucky" and determine the encryption key in a reasonable amount of time, they would only gain access to the data in a single WEDDS transmission.

Fine Grain Access Control—While not included in the Mars Polar Land implementation, the design of WEDDS supports user by user and file by file access control. Specific subsets of the data can be marked for delivery to certain users, and write access can be restricted to allow only particular users access to specific directories.

Minimal Impact to Operations Center Security—In September 1999, a formal peer review of WEDDS was held which included a panel of JPL security experts to determine the readiness of WEDDS for inclusion in the Mars Polar Lander mission. All of the experts in attendance agreed that the impact of WEDDS on the overall security of the mission operations center at UCLA would be insignificant. Furthermore, in the unlikely event that an unauthorized user was able to compromise the WEDDS server, they would not gain login access or write access outside of a specific set of directories. It is not possible for a hacker to use WEDDS to execute malicious code on a mission computer or create a new account for further hacking. In addition, since any incursion would likely consist of a hacker compromising a legitimate user's digital certificate file and password, detection of hackers can be made more likely through two techniques:

1. Keep users informed of the usage of their account.
2. Raise an alert if a user is delivered the same data more than once.

Bandwidth Efficiency—WEDDS delivers data to remote users in compressed packages that contain many files. This is the most efficient way possible to deliver large amounts of data. In addition, since all of the data is transferred to the user at once, the user never needs to be sent the data again. In fact, after receiving the data, the user need not connect to the Internet until additional updates are desired.

Transparency—A remote user's WEDDS client periodically checks with the WEDDS server to determine if new data has become available. If new data is available, the WEDDS client automatically negotiates a secure connection, downloads the compressed packages, and decompresses them on the user's computer into the proper directories. The user doesn't need to do anything for this process to occur—in fact, the user doesn't even need to be present. This means that quite often, new data will arrive while the user is otherwise busy, never requiring the user to initiate the transfer and wait for its completion.

Platform Independence—WEDDS is written in Java, which compatible with nearly every major platform, including SGI, SUN, DEC, Windows 95/98/NT, and Macintosh with no modification.

Multiple Application Support—Since WEDDS, in its simplest form, works by transferring files to and from remote users and the mission operations center, nearly any existing mission application will be able to use WEDDS to operate in a distributed fashion with only minor modifications to WEDDS and the application. For instance, a planning tool that reads in image files and saves command files can run in multiple locations without any major modifications. WEDDS simply needs to be set up to deliver the images to remote users and return their command files to the mission operations center.

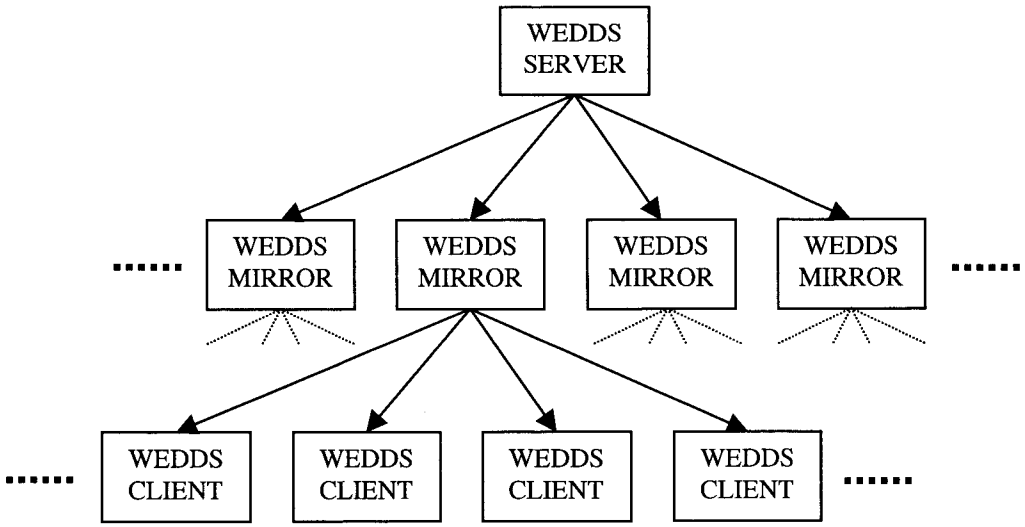

Figure 3 A pyramid distribution system to handle large numbers of users

Scalability—After a user has followed the necessary steps to receive a digital certificate file from the NASA PKI, the mission system administrator simply needs to add the user's full X.500 distinguished name to the list of WEDDS' authorized remote users. As the number of remote users grows very large, WEDDS' performance gracefully degrades. It never needs to send data more than once to a specific user, and it can easily be instructed to limit the number of concurrent transfers. Furthermore, WEDDS' design allows for the construction of a pyramid distribution structure of WEDDS mirrors, shown in figure 3. Each layer of the pyramid is only responsible for delivering data to a fixed number of users or mirrors, so transfers are always completed quickly. A propagation delay exists from the top to the bottom of the pyramid, but it is unlikely that the pyramid would ever need to be more than a few levels deep to support a very large number of users. This capability may be developed further when WEDDS is used to support a major public outreach program for the Mars Polar Lander mission.

7. CONCLUSIONS

WEDDS has successfully accomplished its intended goal: it is capable, in conjunction with existing mission applications, of supporting secure distributed mission operations over the Internet. Missions using this system would be able to avoid using costly leased-line networks, or would use these mediums more securely and efficiently. Distributed operations allow a mission to draw upon the expertise of scientists from all over the world without having to bring them to the mission operations center, greatly improving mission performance while decreasing cost.

Further work is necessary to develop WEDDS into a system that could support mission after mission without any modification. There are also numerous commercial applications of WEDDS that could be considered, from distributing software updates to remote users to automatic mirroring of large databases. Other development work on WEDDS will likely be devoted to automatic detection of new downlink data at the server and improved tolerance of network problems during file transfers.

REFERENCES

[1] Paul Backes, Jeffrey S. Norris, Jeffrey Slostad, Robert Bonitz, Kam Tso, and Greg Tharp, "Mars Polar Lander Mission Distributed Operations," *IEEE Aerospace 2000,* March 2000.

[2] G.C. Omidyar and T.E. Butler, "Analysis of NASA communications (Nascom) II network protocols and performance", *IEEE Telecommunications Conference*, 170-176 vol.1, 1991.

[3] M.J. Wiener, "Performance Comparison of Public-Key Cryptosytstems," *CryptoBytes,* 3(3): 1-5, 1998.

[4]Entrust/Toolkit Java Edition, http://developer.entrust.com/java/, Entrust Technologies, 1999.

[5] SSL 3.0 Spec. http://home.netscape.com/eng/ssl3/. Netscape Corporation.

[6] W. Diffie and M.E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, IT-22: 644-654, 1976.

[7] R.L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, 21(2): 120-126, February 1978.

[8] RSA Labs FAQ, Section 3.2: DES, http://www.rsasecurity.com/rsalabs/faq/3-2.html, RSA Security Incorporated, 1999.

Jeff Norris *is a computer scientist and member of the technical staff of the Autonomy and Control Section at the Jet Propulsion Laboratory. He specializes in software engineering for telerobotics, distributed operations, machine vision, and large scale interfaces. He received his Bachelor's and Master's degrees in*

Electrical Engineering and Computer Science from MIT. While an undergraduate, he worked at the MIT Media Laboratory on data visualization and media transport protocols. He completed his Master's thesis on face detection and recognition at the MIT Artificial Intelligence Laboratory. He now lives with his wife in Azusa, California.

***Paul Backes** is a technical group leader in the Automomy and Control section at the Jet Propulsion Laboratory, Pasadena, CA, where he has been since 1987. He received the BSME degree from U.C. Berkeley in 1982, and MSME in 1984 and Ph.D. in 1987 in Mechanical Engineering from Purdue University. He is currently responsible for distributed operations research for Mars lander and rover missions at JPL. Dr. Backes received the 1993 NASA Exceptional Engineering Achievement Medal for his contributions to space telerobotics (one of thirteen throughout NASA), 1993 Space Station Award of Merit, Best Paper Award at the 1994 World Automation Congress, 1995 JPL Technology and Applications Program Exceptional Service Award, 1998 JPL Award for Excellence and 1998 Sole Runner-up NASA Software of the Year Award. He has served as an Associate Editor of the IEEE Robotics and Automation Society Magazine.*